REVISED STUDY AND EVALUATION SCHEME

FROM

1st TO IVth SEMESTER

MASTER OF ENGINEERING PROGRAMME

REGULAR AND MODULAR PROGRAMME

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

OFFERED BY

PANJAB UNIVERSITY, CHANDIGARH

(Examination 2019-2020)

Scheme of Evaluation (Semester-wise)
M.E. (Computer Science &Engineering (Cyber Security))
(Examination 2019-2020)

1. Duration of the Programmes

i) For Regular M.Tech./M.E. Programmes

The normal duration of M.Tech./ME programmes including Dissertation will be 2 academic years (4 semesters). The maximum period of completion of the programme including Dissertation shall be 3 academic years (6 semesters).

ii) For Modular M.Tech. /M.E. Programmes

The normal duration of Modular M.Tech./M.E. Programmes including Dissertation will be 3 academic years, (6 spells, each spell of 5 weeks duration including Saturdays/ &Sundays). The maximum period of completion of the programme including Dissertation shall be 5 academic years (10 spells).

Scheme for ME CSE (Cyber Security)

First Semester

Sr. No	Course No.	Course Title	Hours / Week	Credits	University External Marks	Internal Sessional Marks	Total
1.	CSN 8101 (Common with CS 8101)	Advance Algorithms	4	4	50	50	100
2.	CSN 8102 (Common with CS 8103)	Advance Computer Networks	4	4	50	50	100
3.	CSN 8103	Cloud Computing and Big Data	4	4	50	50	100
4.	Programme Elective – I		4	4	50	50	100
5.	Programme Elective – II		4	4	50	50	100
6.	CSN 8150	Software Lab-I	4	2	-	100	100
Total			24	22	250	350	600

Elective-I Bucket

CSN 8104 Cyber Forensics
CSN 8105 Information Security

Elective –II Bucket

CSN 8106 Cyber Laws and IPR
(Common with CS 8305)
CSN 8107 Digital Forensics and Incident Response

Second Semester

Sr. No	Course No.	Course Title	Hours / Week	Credits	University External Marks	Internal Sessional Marks	Total
1	CSN 8201 (Common with CS 8202)	Research Methodology	4	4	50	50	100
2	CSN 8202 (Common with CS 8203)	Soft Computing	4	4	50	50	100
3	CSN 8203	Mobile, Wireless and VoIP Security	4	4	50	50	100
4	CSN 8250	Software Lab-II	6	3	-	100	100
5	Programme Elective – III		3	3	50	50	100
6	Programme Elective –IV		3	3	50	50	100
7.	Seminar-I Research Seminar		2	1	-	100	100
Total:			26	22	250	450	700

Elective-III Bucket

CSN 8204 Pattern Recognition and Machine Learning
CSN 8205 Information Retrieval
(Common with CS 8304)

Elective –IV Bucket

CSN 8206 Internet of Things Security
CSN 8207 Social Network Analysis

Third Semester

Sr. No.	Course No.	Course Title	Hours / Week	Credits	University External Marks	Internal Sessional Marks	Total
1	CSN 8301		3	3	50	50	100
2	CSN 8302		3	3	50	50	100
3	CSN 8350 Preliminary Dissertation Work		20	10	--	100	100
Total			26	16	100	200	300

MOOC-I and II Courses

* Students can do credit course of their interest related to Cyber Security on NPTEL, Swayam, etc.

Fourth Semester

Sr. No.	Course No.	Course Title	Hours / Week	Credits	University External Marks	Internal Sessional Marks	Total
1	CSN 8450 Dissertation		25	15	100	100	200
Total			25	15	100	100	200

Instructions for Examiners to award marks/grades for Dissertation:-

S. No.	Grade	Condition
1	**A+**	**Publication from Dissertation in SCI indexed journal.**
2	**A**	**Publication from Dissertation in Scopus indexed journal.**
3	**B+**	**Publication from Dissertation in Proceedings of Conference which is Scopus indexed.**
4	**B**	**Presented paper in International Conference.**
5	**C+**	**Presented paper in National Conference.**

Branch: Computer Science and Engineering

Title	**ADVANCE ALGORITHMS**		**Credits**	04
Code	**CSN 8101**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites	ADA		**Contact Hours**	45
			Time	4 Hours
Objectives	This course will provide the in-depth knowledge of different algorithm design methodologies and the various research concepts involved			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A

Models of Computation and Algorithms Stored program model, Random Access Machines and Turing machines, Algorithms and their complexity, Performance analysis: - Time and space complexity, asymptotic notation. Analyzing recursive algorithms using recurrence relations: Substitution method, Recursion-tree method, Master method.	7
Divide and Conquer, and Greedy Algorithm Design Methodologies Introduction, Quick sort, Strassen's matrix multiplication, Minimum spanning tree, Single source shortest path problem and their performance analysis.	8
Branch-and-Bound, and Lower Bound Theory Introduction, 0-1 knapsack problem, Traveling salesman problem, comparison trees for sorting, searching and merging.	7

SECTION-B

Dynamic Programming and Backtracking Algorithm Design Methodologies Introduction, Traveling salesperson problem, Knapsack problem, multistage graphs, Floyd-Warshall algorithm, N-Queens problem, and their performance analysis.	7
Parallel Random Access Machine Algorithms Introduction, computation model, fundamental techniques and algorithms, selection, sorting, merging, graph problems.	6
Advanced String Matching Algorithms Naïve string matching algorithm, Robin-Karp algorithm, string matching with finite automata, Knuth-Morris-Pratt algorithm.	5
P, NP and Approximation Algorithms Basic Concepts, Non Deterministic algorithms, NP-Complete and NP-hard classes, introduction to approximation, absolute approximations, polynomial time approximation schemes.	5

Suggested Books

1. Cormen, Leiserson, Rivest and Stein: Introduction to algorithms, Prentice-Hall of INDIA.

	2. Horowitz, Sahni and Rajsekaran: Fundamentals of Computer Algorithms, Galgotia. 3. Aho, Hopcroft, Ullman: The Design and analysis of algorithms", Pearson Education.	

Branch: Computer Science and Engineering

Title	**ADVANCE COMPUTER NETWORKS**		**Credits**	04
Code	**CSN 8102**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites	Computer Networks		**Contact Hours**	45
			Time	4 Hours
Objectives	Upon completion of this course, participants will have gained knowledge of computer network concepts and the following: • Fundamentals of IPv6 and MobileIPv6 • Application and importance of Software Defined Networks • Fundamentals of Mobile Computing and related technologies • Basic concepts of Cellular networks and working of GSM, GPRS, 3G and 4G Understanding architecture, application and challenges of MANET, VANET and WSN			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Introduction: Overview of Computer Networks, ISO-OSI and TCP/IP reference models, MAC protocols for LANs, Gigabit Ethernet, Wireless LAN	6
IPv6: Overview of IP and IPv4, **IPv6**: Basic protocol, Extensions and options, Tunneling, Addressing, Neighbor Discovery, Auto-configuration, IPv6 in an IPv4 Internet Migration and Coexistence, **Mobile IPv6**: Overview, Route Optimization, Handover and its impacts on TCP and UDP, Security requirements.	10
Transport Layer: Conventional TCP, TCP extensions for wireless networks	3
Software Defined Networks: Introduction, Evolution and Importance of SDN, Control and Data Planes, Role of SDN Controllers, Application areas of SDN.	5
SECTION-B	
Mobile Computing: Introduction, Mobile Computing Architecture, Technologies: Bluetooth, RFID, WiMAX, Security Issues in Mobile Computing.	5
Cellular Technologies: **Cellular Concept:** Introduction, Frequency Reuse, Channel Assignment, Handoff Strategies, Interference, Cell Splitting and Sectoring. **GSM**: GSM-services, features, system architecture, **GPRS**: Introduction, network architecture, data services, applications and limitations, 3G and 4G.	8
Ad Hoc Networks: Introduction to Adhoc networks, Issues in Adhoc networks and Pro-active and Reactive routing protocols. VANETS: Introduction, architecture, applications and challenges WSNs: Introduction, architecture, applications and challenges.	8

Suggested Books

1. Behrouz A. Forouzan: Data Communications and Networking, 2nd Edition, McGraw-Hill.
2. Andrew S. Tanenbaum, David J. Wetherall: Computer Networks, Pearson.
3. Hesham Soliman: Mobile IPv6 Mobility in Wireless Internet, Pearson Education.
4. Thomas D. Nadeau, Kengray: Software Defined Networks, O'Reilly.

	5. Ashok K. Talukdar: Mobile Computing- Technology, Applications and Service Creation, 2nd Edition, McGraw-Hill. 6. Theodore S. Rappaport: Wireless Communications Principles and Practice, Prentice Hall. 7. Hannes Hartenstein, Kenneth Laberteaux: VANET Vehicular Applications and Inter-networking Technologies, Wiley. 8. Kazem Sohraby, Daniel Minoli, Taieb Znati: Wireless Sensor Networks-Technology, Protocols and Applications, Wiley. 9. Requests for Comments (RFCs) & Internet Drafts, published by Internet Engineering Task Force (www.rfc-editor.org).
Course Outcomes	On completion of this course, a student must be able to 1. Compare ISO-OSI and TCP/IP reference models. 2. Analyze MAC protocols for wired and wireless LANs 3. Understand basic protocol, extensions and security parameters of IPv6. 4. Identify issues in Mobile IPv6. 5. Understand TCP extensions for wireless networks. 6. Understand the concept of Software-Defined Network technology and its Applications. 7. Develop a clear understanding of mobile computing. 8. Understand the process of calling and handover in cellular networks. 9. Understanding working of GSM and GPRS. 10. Develop a critical mind for constructing an adhoc wireless network and various routing protocols for adhoc wireless network. 11. Understanding architecture of VANETs and WSNs.

Branch: Computer Science and Engineering

Title	**CLOUD COMPUTING AND BIG DATA**		**Credits**	04
Code	**CSN 8103**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	Objective of this course is to understand the advantages, challenges, security issues of cloud computing and interrelationships between cloud computing and big data.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Cloud Computing Fundamentals: What Cloud Computing, Essential Characteristics, Architectural Influences, Technological Influences.	6
Cloud Computing Architecture: Cloud Delivery Models, Cloud Deployment Models, Expected Benefits.	10
Cloud Computing Software Security Fundamentals: Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, Secure Cloud Software Requirements.	3
Cloud Computing Risk Issues: Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks,	5
SECTION-B	
Cloud Computing Security Challenges: Security Policy Implementation, Virtualization Security Management, VM Security Recommendations, VM-Specific Security Techniques.	5
Cloud Computing Security Architecture: Architectural Considerations, Identity Management and Access Control, Autonomic Security.	8
Data storage in the cloud: Understanding cloud-based data storage, cloud-based backup system, Understanding File storage, Industry specific cloud-based data storage, Cloud-based database solutions, Cloud-based block storage.	4
Collaboration in the cloud: Web based collaborations, Collaborating via web Logs(Blogs), Using social media for collaboration, Using streaming video content to collaborate.	4

Suggested Books	1. Kris Jamsa, Cloud Computing, Jones & Bartlett,2012 2. Russell Dean Vines and Ronald L. Krutz ,Cloud Security: A Comprehensive Guide To Secure Cloud Computing, Wiley India Pvt Ltd, 2010 3. Barrie Sosinsky, Cloud Computing Bible, Wiley India, 2011
Course Outcomes	At the end of this course, students will be able to:

	• Explain the core concepts of the cloud computing paradigm: how and why this paradigm shift came about, the characteristics, advantages and challenges brought about by the various models and services in cloud computing. • Apply the fundamental concepts in datacenters to understand the tradeoffs in power, efficiency and cost. • Identify resource management fundamentals, i.e. resource abstraction, sharing and sandboxing and outline their role in managing infrastructure in cloud computing. •Illustrate the fundamental concepts of cloud storage and demonstrate their use in storage systems such as Amazon S3 and HDFS. • Analyze various cloud programming models and apply them to solve problems on the cloud.

Branch: Computer Science and Engineering

Title	**CYBER FORENSICS**		**Credits**	04
Code	**CSN 8104**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	Societal and legal impact of computer activity: computer crime, intellectual property, privacy issues, legal codes; risks, vulnerabilities, and countermeasures; methods and standards for extraction, preservation, and deposition of legal evidence in a court of law.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Introduction to Computer Forensics: computer crimes, evidence, extraction, preservation, etc. Overview of hardware and operating systems: structure of storage media/devices; windows/Macintosh/ Linux -- registry, boot process, file systems, file metadata.	6
Data recovery: identifying hidden data, Encryption/Decryption, Steganography, recovering deleted files. Digital evidence controls: uncovering attacks that evade detection by Event Viewer, Task Manager, and other Windows GUI tools, data acquisition, disk imaging, recovering swap files, temporary &cache files.	8
Computer Forensic tools: Encase, Helix, FTK, Autopsy, Sleuth kit Forensic Browser, FIRE, Found stone Forensic ToolKit, WinHex, Linux dd and other open source tools.	8
SECTION-B	
Network Forensic: Collecting and analyzing network-based evidence, reconstructing web browsing, email activity, and windows registry changes, intrusion detection, tracking offenders, etc.	6
Mobile Network Forensic: Introduction, Mobile Network Technology, Investigations, Collecting Evidence, Where to seek Digital Data for further Investigations, Interpretation of Digital Evidence on Mobile Network.	6
Software Reverse Engineering: defend against software targets for viruses, worms and other malware, improving third-party software library, identifying hostile codes-buffer overflow, provision of unexpected inputs, etc.	6
Computer crime and Legal issues: Intellectual property, privacy issues, Criminal Justice system for forensic, audit/investigative situations and digital crime scene, investigative procedure/standards for extraction, preservation, and deposition of legal evidence in a court of law.	5

Suggested Books

TEXT BOOKS

S. No.	NAME	AUTHOR(S)	PUBLISHER
1	Digital Forensics with Open Source Tools. ISBN: 978-1-59749-586-8,	Cory Altheide and Harlan Carvey,	Elsevier publication, April 2011
2	Computer Forensics and Cyber Crime: An Introduction	Marjie T. Britz	(3rd Edition) by, 2013
3	Network Forensics: Tracking Hackers Through Cyberspace,	Sherri Davidoff, Jonathan Ham	Prentice Hall, 2012

	4	Guide to Computer Forensics and Investigations	B. Nelson, A. Phillips, F. Enfinger, C. Steuart.	(4th edition). ISBN 0-619-21706-5, Thomson, 2009.
	5	Cyber Cops, Cyber Criminals& Internet	Keith Merill& Deepti Chopra	(IK Inter.)
Course Outcomes	To understand the various cyber laws those govern the cyber space. To understand the legal aspects of e-commerce. To understand the Intellectual Property Rights and the different components of the IT Act.			

Branch: Computer Science and Engineering

Title	**INFORMATION SECURITY**		**Credits**	04
Code	**CSN 8105**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	The main objectives of this course are: The course will incorporate the foundational understanding of Information Security. The course will incorporate the threats and network perimeter security design principles and provide abilities to review procedures for installation, troubleshooting and monitoring of network devices to maintain integrity, con0fidentiality and availability of data and devices.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Introduction: Security mindset, Computer Security Concepts (CIA), Threats, Attacks, and Assets	6
Cryptographic Protocols - Introduction to Protocols, Communications using Symmetric Cryptography, Substitution Ciphers and Transposition Cipher, Block cipher, Stream cipher, Modes of operation, Symmetric and Asymmetric cryptography.	8
Information Security Threats: Virus,Malware,DDoSattack,Trojan,Worm,Spyware,SocialEngineering,Phishing attacks, man-in-middle attack, DNS poisoning **Vulnerabilities:** Port Scanning, Fingerprinting, Packet Sniffing, Services, Code.	8
SECTION-B	
Proxy & Firewalls WorkingofStatefulFirewall,TheConceptofState,StatefulFilteringandStateful Inspection, Fundamentals of Proxying, Pros and Cons of Proxy Firewalls, Types of Proxies, Tools for Proxying	6
Security Considerations Firewalls Policy, VPN Basics, IPSec Basics, packet filter, stateful firewalls, application level firewalls.	6
Network Intrusion Detection & Prevention Systems Network Intrusion Detection Basics, the Roles of Network IDS in a Perimeter Defence,IDSSensorPlacement,IPS,IPSLimitations,NIPS,Host-BasedIntrusion Prevention Systems, Traffic Monitoring.	6
Security Procedures: Security Policy, Securing the perimeter, physical security, securing the network, securing devices, securing applications, OSUpdates **Common Ways ToProtect Data:** File and folder permissions, encryption, group policy. **Protocol Standards:** SSL/TLS/ SSH/ IPSEC, Kerberos, S/Key, PKI: X.509, PGP.	5

Suggested Books	W. Stallings, Network Security Essentials (3rd Edition), Prentice Hall, W. R. Stevens, TCP/IP Illustrated, Vol. 1: TheProtocols, Addison-Wesley D. E. Comer, Internetworking with TCP/IP, Vol.1 (4th Edition),Prentice Hall, R. Oppliger, Internet and Intranet Security (2nd edition), Artech House, W.R.Cheswick and S.M.Bellovin ,Firewalls and Internet security(2nd edition), Addison-Wesley,

Course Outcomes	Apply fundamental concepts of Information Security threats and vulnerabilities to adopt right security measures and design real time scenarios Design and implement AAA and IPSec and firewall technologies and design network policies to securing networks Design/develop/ implement the security solution for a given application.

Branch: Computer Science and Engineering

Title	**CYBER LAWS AND IPR**		**Credits**	04
Code	**CSN 8106**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	To introduce the Cyber laws and Intellectual property rights.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A

Basics of Computer & Internet Technology Internet, ISP & domain name; Network Security; Encryption Techniques and Algorithms; Digital Signatures	8
Introduction to Cyber World Introduction to Cyberspace and Cyber Law; Different Components of cyber Laws; Cyber Law and Netizens.	3
E-Commerce Introduction to E-Commerce; Different E-Commerce Models; E-Commerce Trends and Prospects; E-Commerce and Taxation; Legal Aspects of E-Commerce.	7

SECTION-B

Intellectual Property Rights IPR Regime in the Digital Society; Copyright and Patents; International Treaties and Conventions; Business Software Patents; Domain Name Disputes and Resolution.	12
IT Act, 2000, 2008 and Amendments Aims and Objectives; Overview of the Act; Jurisdiction; Role of Certifying Authority; Regulators under IT Act; Cyber Crimes-Offences and Contraventions; Grey Areas of IT Act.	11
Project Work Candidates will be required to work on a project. At the end of the course students will make a presentation and submit the project report.	4

Suggested Books

TEXT BOOKS

S. No.	NAME	AUTHOR(S)	PUBLISHER
1	A Guide to Cyber Laws & IT Act 2000 with Rules & Notification	NandanKamath	Galgotia Publications
2	Cyber Cops, Cyber	Keith Merill& Deepti Chopra	(IK Inter.)

		Criminals& Internet		
	3	Information Technology Laws	Diane Row Land	TATA McGraw Hill
	4	Handbook of Cyber Law	Vakul Sharma	(McMillian)
Course Outcomes	1. To understand the various cyber laws those govern the cyber space. 2. To understand the legal aspects of e-commerce. 3. To understand the Intellectual Property Rights and the different components of the IT Act.			

Branch: Computer Science and Engineering

Title	**DIGITAL FORENSICS AND INCIDENT RESPONSE**		**Credits**	04
Code	**CSN 8107**	**Semester:** - 1st	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	Aim of this course is to teach deep understanding of security issues and digital forensics & incident response. In addition, this course also provides the students with specialist knowledge and experience of various digital forensics techniques and incident response.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Forensics Overview: Computer Forensics Fundamentals, Benefits of Computer Forensics, Computer Crimes, Computer Forensics Evidence and the Courts, Legal Concerns and Privacy Issues	11
Forensics Process: Forensics Investigation Process, Securing the Evidence and Crime Scene, Chain of Custody, Law Enforcement Methodologies, Forensics Evidence, Evidence Sources. Evidence Duplication, Preservation, Handling, and Security, Forensics Soundness, Order of Volatility of Evidence, Collection of Evidence on a Live System, Court Admissibility of Volatile Evidence	11
SECTION-B	
Acquisition and Duplication: Sterilizing Evidence Media, Acquiring Forensics Images, Acquiring Live Volatile Data, Data Analysis, Metadata Extraction, File System Analysis, Performing Searches, Recovering Deleted, Encrypted, and Hidden files, Internet Forensics, Reconstructing Past Internet Activities and Events, E-mail Analysis, Messenger Analysis: AOL, Yahoo, MSN, and Chats	12
Mobile Device Forensics: Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3. Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera, Court Testimony, Testifying in Court, Expert Witness Testimony, Evidence Admissibility	11

Suggested Books	1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3rd edition , 2014. 2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005. 3. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Paperback, February 24, 2012. 4. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, 2005.
Course Outcomes	Upon completion of this course, the students will be able to: • Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response. • Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project.

Branch: Computer Science and Engineering

Title	**SOFTWARE LAB-I**		**Credits**	03
Code	**CSN 8150**	**Semester:** -1st	**L T P**	**0 0 4**
Max. Marks	**100**	**Internal:** - 100	**Elective**	N
Pre-requisites	Software testing skills and some testing techniques			
			Time	4 Hours

Branch: Computer Science and Engineering

Title	**RESEARCH METHODOLOGY**		**Credits**	04
Code	**CSN 8201**	**Semester:** - 2nd	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	N
Pre-requisites	Mathematics		**Contact Hours**	45
			Time	4 Hours
Objectives	To make students familiar with various methodologies of research.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Defining Research and Literature Review Need and Significance of Research, Research Process, Different Methods of Research, Different approaches to literature survey, difference between survey and review, Locating and selecting a research problem, Defining a problem statement, formulation of objectives, Retrieving literature from libraries (Online and Offline)	7
Research Design and Methodology Concept of research design, Concept of population and sample, Selection of sample size, Different types of Sampling, Methods of data collection, Concept of data measurement: Nominal, Ordinal, Interval and Ratio, Ethical issues related to data collection, Various Research Data Repositories	5
Statistical Methods of Analysis Descriptive Statistics: Mean, Median, Mode, Range, Standard Deviation, regression and correlation analysis. Inferential Statistics: Estimation of parameters, Hypothesis, Types of Hypothesis, Testing of Hypothesis, Test of Normality, Introduction to Parametric and Non Parametric tests, Test of significance: t-test, chi square test, ANOVA(1-way, 2-way), Repeated Measures ANOVA, ANCOVA, α-correction.	10
SECTION-B	
Introduction to Statistical software SPSS/Minitab/Ms Excel with hands on practical session on concepts detailed in section A3.	5
Procedure for writing a research proposal and research report Purpose , types and Components of research reports, layout of report, Ethical issues related to publishing, plagiarism and self-plagiarism, Introduction to ArXive , BioarXive, Overleaf and Research Gate: Uses and Benefits.	8
Introduction of Software Hands on practical session on software useful for technical report writing such as MS-Word/ Open-Office (reference Management, formatting, Tracking changes, Handling Images and tables layout etc.), Google Docs, Writing document in Latex, Introduction to Mendeley. Graphical presentation of results in different types of graphs and plots.	10
Suggested Books 1. Kothari C.K. (2004) , Research Methodology-Methods and Techniques (New Age International , NewDelhi)2nd Ed. 2. Panneerselvam R., Research Methodology, PHI, 2nd Edition	

	3. N. Gurumani. Scientific Thesis writing and Paper Presentation. MJP Publishers	
Course Outcomes	On completion of the course, the students will be able to 1. Understand the concept of research, identify research problems and learn the basics of literature review. 2. Interpret a good research design and learn the different types of sampling procedures. 3. Write research reports and publications that follow research ethics and standards. 4. Distinguish between data and their methods of measurement and collection. 5. Apply the knowledge of statistical methods of research in their field of study using different statistical softwares.	

Branch: Computer Science and Engineering

Title	**SOFT COMPUTING**		**Credits**	04
Code	**CSN 8202**	**Semester:** - 2nd	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	1.To familiarize with soft computing concepts. 2.To introduce the ideas of Neural networks in applications and research oriented way. 3.To introduce the concepts of Fuzzy logic, Genetic algorithm and their applications to soft computing.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			
SECTION-A				
Introduction: Artificial Intelligence, Artificial Neural Networks, Fuzzy Systems, Genetic Algorithms, Swarm Intelligence Systems, Expert Systems				3
Artificial Neural Networks**:** Classification of ANNs, McCullah Pitts Neuron, Learning Rules, Perceptron, Adaline and Madaline networks, Backpropagation Neural Networks, Kohnen Neural Network, Learning Vector Quantization, Hopfield Neural Networks, Bi-directional Associative Memory.				19
SECTION-B				
Artificial Neural Networks**:** Boltzman Machines Neural Networks, Radial Bias Function Neural Networks, ART.				5
Probabilistic reasoning and Fuzzy Logic: Knowledge representation under uncertainty, Probabilistic reasoning, Bayesian theorem, Bayesian networks, membership functions, fuzzy sets, set operations, fuzzy relations, fuzzy composition, fuzzy interpretation, defuzzification, fuzzy inference system, fuzzy logic applications, neuro-fuzzy systems.				12
Genetic Algorithms: Evolutionary computation. Survival of the Fittest, Fitness Computations, Cross over, Mutation, Reproduction - Rank method - Rank space method etc., solving travelling salesperson problem using GA.				6
Suggested Books	1. Stuart J.Russel, Norvig: AI: A Modern Approach, Pearson Education, Latest Edition. 2. Michael Negnevitsky: Artificial Intelligence: A Guide to Intelligent Systems, 2/E, Addison-Wesley, 2005 3. James Freeman A. and David Skapura M: Neural Networks - Algorithms, Applications & ProgrammingTechniques Addison Wesley, 1992. 4. Yegnanarayana B: Artificial Neural Networks, Prentice Hall of India Private Ltd., New Delhi, 1999 5. Hagan, M.T., Demuth, Mark Beale: Neural Network Design By Cengage Learning			

	6. Goldberg, David E.: Genetic algorithms in search, optimization and machine learning, Latest Edition, Addison Wesley	
Course Outcomes	On completion of the course, a student must be able to 1. Understand the different soft computing concepts. 2. Familiarize with the Artificial Neural networks and their applications. 3. Demonstrate an understanding of the fundamental concepts of Fuzzy logic and Genetic Algorithms and their use in problem solving.	

Branch: Computer Science and Engineering

Title	**MOBILE, WIRELESS AND VOIP SECURITY**		**Credits**	04
Code	**CSN 8203**	**Semester:** - 2nd	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites	Computer Networks		**Contact Hours**	45
			Time	4 Hours
Objectives	This course is designed to address the mobile security, growing threat to mobile devices, networks and services delivered over the mobile infrastructure. This is a graduate-level course that provides an introduction to mobile security. This course is designed with five main goals: • To have knowledge of the base functionality of Wireless, Telecommunication and IP telephony networks, their differences, security vulnerabilities and mitigation techniques used to secure the systems from attack. • To understand wireless standards, how authentication and encryption works, how wireless networks are vulnerable to security threats and ways to secure the wireless network. • How to utilize different protocols and services to test, verify and mitigate security vulnerabilities on the wireless and mobile network • To understand how network monitoring protocols and programs enable you to discover vulnerabilities to the network devices as well as how to catch attacks in progress and how to identify toll fraud.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Introduction to Mobile Security: Security features in wireless environment, mobile network environment, limitations of mobile environment, mobility and security, attacks in mobile environment, security issues in mobile environment.	7
Mobile Networks: Bluetooth overview, architecture and components, security of Bluetooth, overview of GSM, architecture of the GSM and 3G networks, GSM security features, attacks on GSM and 3G networks security, SMS/MMS, Mobile Geolocation and Mobile Web Security.	8
Next Generation Networks: 4G and 5G Wireless Communications Systems, Wireless Application Protocol (WAP), Protocol Stack and security related issues.	7
SECTION-B	
Security in Wireless Communication: 802.11 Architecture, Wireless LAN Components, security of 802.11 Wireless LANs and security threats, features and requirements, problems with the IEEE 802.11 standard security, emerging security standards and technologies	8
VoIP Systems: Introduction to Voice over IP (VoIP), Voice and Video over IP (Media over IP), Session Initiation Protocol (SIP) and its use in Media over IP, Case Study: Skype/Google.	5
Security in VoIP: Attacks against the VoIP network, DDoS Attacks, challenges against implementing VOIP network, WEP (Wired Equivalent Privacy), Effects of using WEP in VoIP networks, Concepts of WPA and WPA2, SRTP, ZRTP, SSL/TLS, IPSEC.	10

Suggested Books	**TEXT BOOKS**			
	S. No.	**NAME**	**AUTHOR(S)**	**PUBLISHER**
	1	Network Security Essentials, Applications and Standards	William Stallings	Pearson Education
	2	Cryptography & Network Security	B.A. Forouzan	Tata McGrawHill
	3	Voice over IP Networks Quality of Service, Pricing and Security	Pramode K. Verma and Ling Wang	Springer
	RECOMMENDED BOOKS			
	1	Cryptography and Network Security Principles and practice	William Stallings	Pearson Education.
	2	Introduction to Computer Security. Addison-Wesley	Bishop, Matt	Pearson Education, Inc./ ISBN: 0-321-24744-2, 2005
	3	Principles of Information Security	Michael. E. Whitman and Herbert J. Mattord	
	4	Cryptography & Network Security, TMH,	AtulKahate	2nd Edition
Course Outcomes	On completion of the course, a student must be able to understand and apply concepts of mobile, wireless and VoIP security.			

Branch: Computer Science and Engineering

Title	**SOFTWARE LAB-II**		**Credits**	03
Code	**CSN 8250**	**Semester:** - 2nd	**L T P**	**0 0 6**
Max. Marks	**100**	**Internal:** - 100	**Elective**	N
Pre-requisites	Software testing skills and some testing techniques			
			Time	6 Hours

Branch: Computer Science and Engineering

Title	**PATTERN RECOGNITION AND MACHINE LEARNING**		**Credits**	04
Code	**CSN 8204**	**Semester:** - 2nd	**L T P**	4 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites			**Contact Hours**	45
			Time	4 Hours
Objectives	This course provides a broad introduction to machine learning and statistical pattern recognition. It offers some of the most cost-effective approaches to automated knowledge acquisition in emerging data-rich disciplines and focuses on the theoretical understanding of these methods, as well as their computational implications.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A

PATTERN CLASSIFIER : Overview of pattern recognition – Discriminant functions – Supervised learning – Parametric estimation – Maximum likelihood estimation – Bayesian parameter estimation – Perceptron algorithm – LMSE algorithm – Problems with Bayes approach – Pattern classification by distance functions – Minimum distance pattern classifier.	7
UNSUPERVISED CLASSIFICATION Clustering for unsupervised learning and classification – Clustering concept –k-means algorithm – Hierarchical clustering procedures – Graph theoretic approach to pattern clustering – Validity of clustering solutions.	8
FEATURE EXTRACTION AND SELECTION Need for feature extraction and selection, Entropy minimization – Karhunen – Loeve transformation – Feature selection through functions approximation – Binary feature selection. Dimensionality reduction, **Curse of dimensionality,** Principle Component Analysis, Applying PCA	7

SECTION-B

Linear discriminant functions : Gradient descent procedures, Perceptron, Support vector machines Kernel Trick; Various kernels like RBF, Gaussion etc amd their effect, Constructing Kernels	6
Artificial neural networks: Multilayer perceptron - feedforwark neural network. A brief inttroduction to deep neural networks, convolutional neural networks, recurrent neural networks	9
Recent Advances: Neural network structures for Pattern Recognition – Neural network based Pattern associators – Unsupervised learning in neural Pattern Recognition – Self-organizing networks – Fuzzy logic – Fuzzy pattern classifiers – Pattern classification using Genetic Algorithms.	8

Suggested Books

1. Robert J.Schalkoff, Pattern Recognition Statistical, Structural and Neural Approaches, John Wiley & Sons Inc., New York, 1992.
2. Christopher M. Bishop ,Pattern Recognition and Machine Learning,Springer,2006
3. Tom Mitchell,Machine Learning, McGraw Hill, 1997.
4. Petra Perner. Machine Learning and Data Mining In Pattern Recognition, Springer Science & Business Media, 2009

Course Outcomes	On completion of the course, students will be able to CO1: Identify and describe existing pattern recognition and machine learning approaches for different modalities CO2: Identify different data analysis techniques like frequent pattern analysis, classification and clustering CO3 Demonstrate the use of various machine learning techniques on different applications

Branch: Computer Science and Engineering

Title	**INFORMATION RETRIEVAL**		**Credits**	03
Code	**CSN 8205**	**Semester:** - 2nd	**L T P**	3 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites	efficient text indexing, link-based algorithms, and Web metadata		**Contact Hours**	45
			Time	3 Hours
Objectives	This subject will provide the knowledge of various concepts involved in efficient information retrieval that leads to the development of efficient Web crawling techniques.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
Introduction Introduction to Information Retrieval. Inverted indices and boolean queries. Query optimization. The nature of unstructured and semi-structured text.	5
The term vocabulary and postings lists Text encoding: tokenization, stemming, lemmatization, stop words, phrases. Optimizing indices with skip lists. Proximity and phrase queries. Positional indices.	5
Dictionaries and tolerant retrieval Dictionary data structures. Wild-card queries, permuterm indices, n-gram indices. Spelling correction and synonyms: edit distance, soundex, language detection.	6
Index construction Postings size estimation, sort-based indexing, dynamic indexing, positional indexes, n-gram indexes, distributed indexing, real-world issues.	5
SECTION-B	
Scoring Term weighting and the vector space model. Parametric or fielded search. Document zones. The vector space retrieval model. weighting. The cosine measure. Scoring documents.	6
Computing scores in a complete search system Components of an IR system. Efficient vector space scoring. Nearest neighbor techniques, reduced dimensionality approximations, random projection.	6
Classification Naive Bayes models. Spam filtering, K Nearest Neighbors, Decision Trees, Support vector machine classifiers.	6
Web Crawling What makes the web different? Web search overview, web structure, the user, paid placement, search engine optimization. Web size measurement, Crawling and web indexes. Near-duplicate detection, Link analysis, Learning to rank, focused web crawler and its different architectures.	6
Suggested Books	1. C. Manning, P. Raghavan, and H. Schütze: *Introduction to Information Retrieval*, CambridgeUniversity Press,2008

2. R. Baeza-Yates, B. Ribeiro-Neto: *Modern Information Retrieval,* Addison-Wesley, 1999

Branch: Computer Science and Engineering

Title	**INTERNET OF THINGS SECURITY**		**Credits**	03
Code	**CSN 8206**	**Semester:** - 2nd	**L T P**	3 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites	efficient text indexing, link-based algorithms, and Web metadata		**Contact Hours**	45
			Time	3 Hours
Objectives	The objective of the course is to make students aware about the security issues and needs of the IoT systems and enable them to design safe and secure IoT systems.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			

SECTION-A	
The IoT in the enterprise The things in the IoT, The IoT device lifecycle, The hardware, Operating systems, IoT communications, Messaging protocols, Transport protocols, Network protocols, Data link and physical protocols, IoT data collection, storage, and analytics, The IoT of the future and the need to secure	5
Vulnerabilities, Attacks, and Countermeasures The classic pillars of information assurance, Threats, Vulnerability, Risks, Common IoT attack types, Attack trees, Fault (failure) trees and CPS, Fault tree and attack tree differences, IoT attacks: Wireless reconnaissance and mapping, Security protocol attacks, Physical security attacks, Application security attacks, Threat modeling an IoT system	5
Security Engineering for IoT Development Building security in to design and development, Secure design: Safety and security design, Processes and agreements, Technology selection – security products and services	6
The IoT Security Lifecycle Implementation and Integration, Operations and maintenance, dispose	5
SECTION-B	
Cryptographic Fundamentals for IoT Security Engineering Cryptography and its role in securing the IoT, Types and uses of cryptographic primitives in the IoT, Encryption and decryption, Hashes, Digital signatures, Cryptographic key management fundamentals, Key generation, Key establishment, Key derivation, Key storage, Cryptographic controls built into IoT communication protocols, Cryptographic controls built into IoT messaging protocols	6
Introduction to identity and access management for the IoT The identity lifecycle, Establish naming conventions and uniqueness requirements, Credential and attribute provisioning, Account monitoring and control, Account updates, Account suspension, Account/credential deactivation/deletion, Authentication credentials, Passwords,	6

Symmetric keys, Certificates, Biometrics, IoT IAM Infrastructure, Authorization and Access Control	
Cloud Security for the IoT Cloud Services and the IoT, AWS IoT, Microsoft Azure IoT, Cloud IoT Security Controls.	6
Suggested Books	1. Brain Russell and Drew Van Duren, Practical Internet of Things Security, PACKT Publishing. 2. Shancang Li, Li Da Xu, Securing the Internet of Things, Elsevier. 3. Chintan Patel, Nishant Doshi, Internet of Things Security: Challenges, Advances, and Analytics, CRC Press. 4. David Etter, Iot Security: Practical Guide Book, CreateSpace Independent Publishing Platform. 5. Shishir Kumar Shandilya, Soon Ae Chun, Smita Shandilya, Edgar Weippl, Internet of Things Security: Fundamentals, Techniques and Applications, River Publishers

Branch: Computer Science and Engineering

Title	**SOCIAL NETWORK ANALYSIS**		**Credits**	03
Code	**CSN 8207**	**Semester:** - 2nd	**L T P**	3 0 0
Max. Marks	**External:** - 50	**Internal:** - 50	**Elective**	Y
Pre-requisites			**Contact Hours**	45
			Time	3 Hours
Objectives	To learn about structure and evolution of networks, to build a framework of network analysis that covers measures such as density, centrality, clustering, centralization, and spatialization.			
Note for Examiner	The Semester question paper of a subject will be of 50 marks having 7 questions of equal marks. First question, covering the whole syllabus and having questions of conceptual nature, will be compulsory. Rest of the paper will be divided into two parts having three questions each and the candidate is required to attempt at least two questions from each part.			
SECTION-A				
Networks- Concepts: nodes, edges, adjacency matrix, one and two-mode networks, node degree				5
Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment				5
Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization				6
Community- Concepts: clustering, community structure, modularity, overlapping communities				5
SECTION-B				
Small world network models, optimization, strategic network formation and search- Concepts: small worlds, geographic networks, decentralized search				6
Contagion, opinion formation, coordination and cooperation- Concepts: simple contagion, threshold models, opinion formation**,** unusual applications of SNA				6
SNA and online social networks- Concepts: how services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality				6
Suggested Books	1. John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012. 2. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011. 3. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013. 4. David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.			

****